Service Level Agreement

Trinity Cyber

This Service Level Agreement (SLA) is an agreement between Company and Trinity Cyber.

1. SERVICE COMMITMENT

Trinity Cyber is committed to providing effective, reliable, highly accurate file submission services (Services). As a part of this commitment, Trinity Cyber is pleased to offer the following guarantees.

- System Performance Guarantee
- Support Guarantee

2. GUARANTEES

A. SYSTEM PERFORMANCE GUARANTEE

Trinity Cyber's file inspection service technology is designed for high availability, high speed, high accuracy file inspection, and file modificationas a security control.

Availability. Trinity Cyber guarantees 99.9% service availability up to the specified data and file rates averaged across an aggregate of the files submitted over the rolling period of one month. No guarantees are made about individual files or specific file types. Trinity Cyber will proactively monitor itsService as it relates to Company's file submissions to proactively mitigate potential fault conditions.

Processing Latency. Trinity Cyber's processing latency will be measured from the time a complete file is received by a Trinity Cyber file submission server until a response is transmitted in return. It does NOT include any transport latency to or from Trinity Cyber's point of presence, transfer latencies for protocol layers above the data link layer, or latencies introduced due to the dynamic nature of the Internet.

- Trinity Cyber commits to 90% of files getting processed by its file submission service technology in one second or less over a rolling 90-day period, with an average file size of 500KB across all files and a rate of processing 100 files per second per site with a maximum of five sites.
- It is incumbent on Company to adhere to and monitor average file size, data transmission rates, and file submission rates in order to maintain processing optimization of Trinity Cyber's file submission servers and avoid unintentional denial of service.

Accuracy. Provided that Company permits data retention of malicious or suspicious files submitted to the service, then Trinity Cyber will maintain a False Detection Rate[1] (FDR) less than 5% for file inspection, averaged over the course of a rolling 30-day period, and will make reasonable efforts to triage, identify and promptly remediate errors in detection. Should Company believe that false detections are disrupting the availability of other services, Company shall contact Trinity Cyber to request review and remediation, per the terms below. Trinity Cyber will implement new file threat detections on behalf of Company, on a routine and emergency basis, and will maintain the same levels of accuracy and efficacy of these updates prior to deployment to file submission servers. Should Company believe any such update has caused a disruption to its business processes, Company shall contact Trinity Cyber to request review and remediation per the terms below.

B. SUPPORT GUARANTEE

Trinity Cyber will establish and maintain a regular communication channel with personnel from Company and provide reasonable assistance in integrating its File Submission response feed with Company toolsets.

Corrections and Assurances. Trinity Cyber guarantees technical support services will be available to Company through the Trinity Cyber Operations Center, which will operate 24 hours a day, 7 days a week, 365 days a year. Trinity Cyber guarantees that should any latency, availability, or throughput issue be identified by Company and communicated reasonably to Trinity Cyber, Trinity Cyber technicians will review and remediate it according to the routine and emergency timelines set forth herein. Such support shall include answering inquiries regarding the Solution and receiving reports of Errors. Monetary compensation for violations of this SLA will be provided upon review by Trinity Cyber and will

[1] False Detection Rate is calculated as the number of times a false detection occurred divided by the number of times the detection of a particular event was attempted. This value is in sharp contrast to the more commonly used less meaningful False Positive Rate, which is typically calculated as the number of times a false detection occurred divided by the number the times detection processing occurred. The use of a low FPR is more easily achievable and can often lull cyber defenders into a false sense of security.

be proportional to the period impacted and monthly billable cost for the network segment impacted, not to exceed the contract consideration amount for a one-year term.

Requests for Review and Remediation. All routine non-emergency requests for review and remediation of minor service disruption not broadly impacting the general availability of the File Submission service shall be made either in writing, delivered electronically, or via telephone call to Trinity Cyber's Operations Center or to its Client Success Management team at clientsupport@trinitycyber.com.

All routine requests will be reviewed within four (4) hours of receipt and Trinity Cyber will provide an initial summary of findings to engage with Company in the resolution process. An initial remediation will be implemented no later than twenty-four (24) hours after initial contact unless another timeframe is mutually agreed upon by Trinity Cyber and Company.

All *emergency requests* for review and remediation of broad service disruptions generally impacting the availability of Company's network or disruption to its business processes shall be made via telephone call to Trinity Cyber's 24x7 Operations team at (240) 842 -9930.

For emergency requests, Trinity Cyber guarantees that should latency, availability, or throughput issues be identified by Company and communicated reasonably to Trinity Cyber, that Trinity Cyber will respond within fifteen (15) minutes of receiving such notice to initiate troubleshooting and attempt to find a solution. An initial investigation report will be provided within 24 hours and a long-term remediation plan to prevent similar disruptions in the future will be provided within three (3) days.

3. CUSTOMER ACKNOWLEDGMENTS AND RESPONSIBILITIES

Company recognizes that the Internet is a diverse collection of independently operated networks, equipment, and service providers. No attributes of performance described herein that cannot be controlled by Trinity Cyber will be attributed to it. It is incumbent upon Company to also do their due diligence and ensure fail-safes and automated bypass capabilities are in place to mitigate any failures outside the control of either Company or Trinity Cyber.

Trinity Cyber will provide engineering design support and documentation sufficient to ensure Company is comfortable with their recourse options should Trinity Cyber be unable, for reasons outside of their control, to alleviate an availability or performance issue in a timely manner.

4. SERVICE CREDIT CLAIM PROCESS

In order to initiate a claim for Service Credit, Customer must contact Trinity Cyber's Client Success Management team at clientsupport@trinitycyber.com within seven (7) business days after the end of the month for which credit is requested. The Service Credit request must provide: (a) the Customer name and contact information; (b) the date and beginning/end time of the claimed outage or failed metric; and (c) a brief description of the characteristics of the claimed outage or failed metric.